Golay and Other Box Codes

G. Solomon[1]

The (24,12;8) extended Golay Code can be generated as a 6×4 binary matrix from the (15,11;3) BCH-Hamming Code, represented as a 5×3 matrix, by adding a row and a column, both of odd or even parity. The odd-parity case provides the additional 12th dimension. Furthermore, any three columns and five rows of the 6×4 Golay form a BCH-Hamming (15,11;3) Code. Similarly a (80,58;8) code can be generated as a 10×8 binary matrix from the (63,57;3) BCH-Hamming Code represented as a 9×7 matrix by adding a row and a column both of odd and even parity. Furthermore, any seven columns along with the top nine rows is a BCH-Hamming (63,57;3) Code.

A (80,40;16) 10×8 matrix binary code with weight structure identical to the extended (80,40;16) Quadratic Residue Code is generated from a (63,39;7) binary cyclic code represented as a 9×7 matrix, by adding a row and a column, both of odd or even parity.

I. Golay Code Properties

The $(24, 12; 8)$ extended Golay Code possesses many properties. Solomon and Sweet [1] showed that it can be represented by a 6 × 4 binary matrix with equal row and column sums. Certain permutations of the matrix that keep the rows fixed give rise to at least three other boxes or matrices with identical row/column sum properties. These boxes can be used for "eyeball" decoding which avoids algebraic procedures. Here new properties of the extended Golay Code are further demonstrated.

A. Constructions

The (24,11;8) code in 6 × 4 matrix form is obtained from the BCH-Hamming (15,11;3) Code by adjoining row and column even parity. The BCH-Hamming Code here is expressed as a 5 × 3 matrix with entries in the *(i, j)* positions, $0 \leq i \leq 4$, $0 \leq j \leq 2$ corresponding to the coordinates $5i + 3j$ mod 15 of the code.

Let **A** be the BCH-Hamming (15,11;3) Code. The Mattson-Solomon (MS) polynomial for a code word $\mathbf{a} \in \mathbf{A} = (a_i; i = 0 \ldots 14)$ is given by

$$P_{\mathbf{a}}(z) = C_0 + \mathrm{Tr}\, Cz + \mathrm{Tr}\, Dz^3 + Ez^5 + E^2 z^{10}$$

where $C, D \in GF(16)$, $E \in GF(4)$, $C_0 \in GF(2)$, and $P_{\mathbf{a}}(\beta^i) = a_i$ for β a primitive 15th root of unity. Tr denotes the linear operator Trace in $GF(16)$. Tr $a = a + a^2 + a^4 + a^8$.

The parity check polynomial for the code is $(z + 1) \times f_1(z) f_3(z) f_5(z)$ where $f_i(z)$ is the irreducible polynomial over $GF(2)$ with β^i a root.

[1] Independent consultant to the Communications Systems Research Section.

The weight, $w(\mathbf{a}) \bmod 4$ for even-weight words $\mathbf{a}(C_0 = 0)$, is given by $w \bmod 4 = 2\Gamma_2(P_{\mathbf{a}}(x))$ where $\Gamma_2(P_{\mathbf{a}}(x)) = D^5 + D^{10} + E^3$ [2].

Now place the code words in 5×3 matrices (b_{ij}), $0 \le i \le 4$, $0 \le j \le 2$ corresponding to their values $5i + 3j \bmod 15$. The ith coordinate is entered thusly:

0	5	10
3	8	13
6	11	1
9	14	4
12	2	7

The MS polynomial expressed in the 5×3 setting, indexing each row by y in terms of the independent variable x, becomes Tr Dy^3+Tr$'$ $(E'+Cy+C^4y^4)x$; $E' = E^2$. Note again that for the rows, the trace is defined over $GF(4)$ as follows: Tr$'$ $a = a + a^2$ for $a \in GF(4)$.

Form the sum over the rows to give a sixth row with MS polynomial Tr$'$ $E'x$. Form the parity sum over the columns to obtain a 6×1 column, which is of course Tr Dy^3; $y^6 = y$. The bottom row is indexed by $y = 0$, and the parity column corresponds to $x = 0$.

This is what is needed to prove the following results. Note that the coefficient of x is $E' + Cy + (Cy)^4$. This is the MS polynomial for a $(5, 3; 3)$ code indexed by $y^5 = 1$ over $GF(4)$. Adding a sixth row, one obtains a $(6, 3; 4)$ code indexed by $y^6 = y$ over $GF(4)$ as the coefficient of x. Note that the constant term in each row varies and is a $(5, 4; 2)$ binary code. It contributes the same values to the fourth parity column. Thus if one started with a BCH subcode of dimension 10 of even weight w with $w \bmod 4 = 2\Gamma_2$ where $\Gamma_2 = D^5 + D^{10} + E^3$, adjoining the parity rows and columns adjoins row and column code words whose weight modulo 4, $w \bmod 4 = D^5 + D^{10} + E^3$. So the total new weight $w' = 0 \bmod 4$.

This proves $w' \ge 8$. For if one started with $w = 4$, one has either $E^3 = 1$ and $D^5 + D^{10} = 1$, adding weight 4, or $E = 0$ and $D^5 + D^{10} = 0$, giving $D^5 = 1$, adding a column of weight 4.

One could also show easily that $w' \ge 8$ by noting that the coefficient of x is now a $(6, 3; 4)$ code over $GF(4)$, having adjoined an even parity row. Thus there are at least four rows of weight 2 each. The addition of the even parity column ensures $w \ge 8$ when the coefficient of $x = 0$. The new code words are of weights 8, 12, 16, and 24 in the 6×4 matrix code generated. Complementing these new code words still gives words of weights 8, 12, and 16, which takes care of the odd weight Hamming code words adding up to dimension 11.

The 12th dimension of the constructed code is obtained by adding odd parity row and column to the Hamming words. Thus the additional row (first 3 columns) is given by $1 +$ Tr Ex and the additional column (upper 5 rows) is given by $1 +$ Tr Dy. The even weights are determined by $\Gamma_2 = E^3 + D^5 + D^{10}$. Consider the even weights equal to 4 and 6. If $E^3 = 0$ and 1, respectively, then weights 3 and 1, respectively, have been added to the bottom row. If $D^5 + D^{10} = 0$ and 1, respectively, then weights 1 and 3, respectively, have been added to the fourth column. If $D = 0$, then a 5 has been added.

Consider the case of $\Gamma_2 = E^3 + D^5 + D^{10} = 1$ or $w = 6$. Either $E \ne 0$, $D^5 = 1$, and weight 6 is added, or $E = 0$, $D^5 \ne 1$, and weight 2 is added. For $\Gamma_2 = 0$ or $w = 4$, $E \ne 0$ and $D^5 \ne 1$, so weight 4 is added, or $E = 0$ and $D^5 = 1$ and again weight 4 is added. In either case, adding odd parity row and column ensures that $w' = 0 \bmod 4$ and $w' \ge 8$.

This new code has weights 8, 12, 16, and 24. This is sufficient to guarantee that this code is the extended Golay Code by various uniqueness theorems in the literature. However, there is an explicit construction by Solomon and Sweet that does it.

B. The (24,12;8) Code Is the Golay Code

This formulation was first used by Solomon and Sweet [1]. The code has words of weight $w = 0 \bmod 4$ and is thus self-dual, has minimum distance 8, and contains the all one vector. This is the Golay Code. In fact, the correspondence between the coordinates of the cyclic code generated by the parity check polynomial and its representation as a 6×4 binary matrix is

0	2	1	3
4	12	7	10
9	22	6	11
16	15	8	19
20	21	18	13
17	∞	5	14

C. Encoding

Let $\mathbf{a}$ be a code word of length 24: $\mathbf{a} = (a_0, a_1, a_2, \ldots, a_{22}, \infty)$. Label positions $(0, 1, 2, \ldots, 22, \infty)$ generated by the recursion shift register rule

$$f(x) = x^{12} + x^{10} + x^7 + x^4 + x^3 + x^2 + x + 1$$

$$a_{n+12} = a_{n+10} + a_{n+7} + a_{n+4}$$

$$+ a_{n+3} + a_{n+2} + a_{n+1} + a_n$$

where $n = 0, 1, 2, 3, \ldots, 22$ and $a_\infty = \sum_{i=0}^{22} a_i$.

D. A Key Property

Theorem. Represent the Golay Code as a 6×4 binary matrix and consider any 5×3 submatrix obtained by removing one column and one row. This is a BCH-Hamming (15,11;3) Code. There is one proof and one verification.

Proof: Consider the 6×4 matrix with the top row deleted. Using the bottom parity check row and considering the first three columns, there is now a permuted 5×3 BCH-Hamming Code where the rows have been interchanged.

Note that the coefficient of x is the $(6, 3; 4)$ extended Reed-Solomon (RS) Code over $GF(4)$, which gives rise to the $(24, 6; 8)$ portion of the code. The map $y \rightarrow (1 + \alpha y + \alpha^2 y^4)$ is a permutation of this code that interchanges the top and bottom rows corresponding to $y = \beta^0 = 1$ and $y = 0$. For $\alpha = \beta^5$ a root of $x^2 + x + 1$, the second and fifth rows are interchanged and the third and fourth rows are fixed. Here y ranges over the values $y^6 = y$.

The remaining five dimensions, which are a function of C_0 and D in the BCH-Hamming Code, are easily seen to be manipulated so the weights stay the same. Since the code is clearly invariant under cyclic row cyclic permutations, this takes care of all subcodes with the first three columns fixed.

Now interchange the first column with the fourth rightmost parity column and the second with the third to obtain a BCH-Hamming Code still like the above in the top five rows. This interchange of columns is given by $x \rightarrow x + 1$.

This map takes the row indexed by y, Tr Dy+Tr$'$ $(E'+Cy+(Cy)^4)x$, into a permuted row indexed by y, where $D \in GF(16)$ has been augmented: Tr$'$ $(E'+Cy+(Cy)^4)+$ Tr $Dy+$Tr$'$ $(E'+Cy+(Cy)^4)x$. There clearly exists a D' such that $D' =$ Tr$'$ $(E'+Cy+(Cy)^4)+$Tr Dy for all values of y. Now clearly every three columns that occurred in the leftmost 5×3 matrix now occur in the newly formed 5×3 matrix. As the code is invariant under cyclic column permutation, the proof is complete. ❐

Verification: Postconjecture and preproof, a computer verification was performed by F. Pollara; this verification generated the identical weight distributions of the Hamming Code for each relevant permutation.

II. Extension of Results to (63,57;3) BCH-Hamming Code

Starting with the BCH-Hamming Code of length 63 in its 9×7 setting and using the MS polynomials for codes of lengths 63, 9, and 7, one obtains a 10×8 code of distance 8.

A. MS Polynomial for the BCH-Hamming Code in a 9 x 7 Setting

Let $f_1(x) = x^6 + x + 1$ be the primitive polynomial with β as a root. Then $f_i(x)$ is the irreducible polynomial with coefficients in $GF(2)$ with β^i as a root.

The BCH-Hamming Code in its MS polynomial form is written as

$$P(z) = C_0 + \sum \text{Tr } C_i z^i + \sum \text{Tr}' \; C_j z^j + C_{21} z^{21} + C_{21}^2 z^{42}$$

where $C_i \in GF(64)$; $i = 1, 3, 5, 7, 11, 13, 15, 23$; $C_j \in GF(8)$; $j = 9, 27$; and

$$\text{Tr}' \; a = a + a^2 + a^4; \; a \in GF(8)$$

Let $z \in GF(64)$ be a primitive root of $GF(64)$. Express $z = xy$ where

$$x = \beta^{9i}, \; 0 \leq i \leq 6; \; y = \beta^{7j}, \; 0 \leq j \leq 8$$

then

$$\text{Tr } Cz = \text{Tr } Cxy = \text{Tr}' \; [Cy + (Cy)^8]x$$

$$\text{Tr } C_3 z^3 = \text{Tr}' \; [C_3' y^6 + C_3'^8 y^3] x^6$$

$$C_3' = C_3^2$$

Replacing the letter by its primed letter to indicate a missing appropriate power,

$$\text{Tr } C_5 z^5 = \text{Tr}' \ (C'_5 y^2 + C'^8_5 y^7) x^6$$

$$\text{Tr } C_7 z^7 = \text{Tr} C'_7 y \text{Tr } C_9 z^9 = \text{Tr}' \ C'_9 x$$

$$\text{Tr } C_{11} z^{11} = \text{Tr}' \ (C'_{11} y^4 + C'^8_{11} y^5) x$$

$$\text{Tr } C_{13} z^{13} = \text{Tr}' \ (C_{13} y^4 + C^8_{13} y^5) x^6$$

$$\text{Tr } C_{15} x^{15} = \text{Tr}' \ (C'_{15} y^3 + C'^8_{15} y^6) x$$

$$\text{Tr } C_{23} z^{23} = \text{Tr}' \ (C'_{23} y^2 + C'^8_{23} y^7) x$$

$$\text{Tr } C_{27} z^{27} = \text{Tr}' \ C_{27} x^6$$

$$C_{21} z^{21} = C_{21} y^{21}$$

Recall that the Golay Code can be viewed in the MS polynomial formulation for lengths 6 or 4 as made up of components that are themselves RS Codes. Similarly express the Hamming Code here in MS polynomials of lengths 9 or 7. Recall that a binary codeword of length 7 has an MS polynomial of the form

$$P(x) = C_0 + \text{Tr}' \ (Cx + Dx^6)$$

$$\text{Tr}' \ C = C + C^2 + C^4; \ C \in GF(8)$$

Write the BCH-Hamming Code in all 57 dimensions as

$$C_0 + \text{Tr } C'_7 y^7 + C'_{21} y^{21} + C'^2_{21} y^{42}$$

$$+ \text{Tr}' \ (C'_9 + Cy + C^8 y^8 + C'_{11} y^4 + C'^8_{11} y^5$$

$$+ C'_{15} y^3 + C'^8_{15} y^6 + C'_{23} y^2 + C'^8_{23} y^7) x$$

$$+ \text{Tr}' \ (C_{27} + C'_3 y^6 + C'^8_{11} y^3 + C'_5 y^2$$

$$+ C'^8_5 y^7 + C_{13} y^4 + C^8_{13} y^5) x^6$$

where $C_i \in GF(64)$, $i = 1, 3, 5, 7, 11, 13, 15, 23$; $C_j \in GF(8)$; $j = 9, 27$.

Note that the coefficient of x in the above expression is a (9,9;1) code over $GF(8)$, the coefficient of x^6 is a (9,7;3) RS code over $GF(8)$. The values $C_0 + \text{Tr } C'_7 y^7 + C'_{21} y^{21} + C'^2_{21} y^{42}$ taken over y form a (9,9;1) binary code. The minimum weight of this code is clearly 3. If the coefficient of x^6 is zero, then the minimum weight is given by a weight one word (coefficient of x) in the (9,9,1) code (giving rise to a weight 4 word) complemented by a value of C_0, which is 1 at that y position. If the coefficient of x^6 is nonzero, one again has a minimum weight 3 word.

Now extend the 9×7 matrix to 10×8 by adjoining even parity rows and columns. The 10th parity row is clearly the code word in MS form $C_0 + \text{Tr}' \ (C_9 x + C_{27} x^6)$. The coefficients $C_0 + \text{Tr } C'_7 y^7 + C'_{21} y^{21} + C'^2_{21} y^{42}$ in the row MS polynomials for $y^{10} = y$ now form a $(10, 9; 2)$ binary code. The coefficient of x is also a $(10, 9; 2)$ code over $GF(8)$. The coefficient of x^6 is a $(10, 7; 4)$ code over $GF(8)$. Adding the even parity column guarantees that the minimum weight w of the expanded code $w = 8$.

Thus the BCH-Hamming Code extends to a $(80, 57; 8)$ code. Finally, if the 10th row and 8th column are to be of odd parity, the minimum weight still is 8. It is obvious that the weight does not decrease this way. Consider words of weight $w \leq 7$ and try placing them in a 9×7 setting. Clearly $10 - w$ columns are at least zero and odd parity will certainly increase the weight this much.

B. BCH-Hamming Submatrices of the 10 x 8 Code

To show that every 9×7 submatrix of the 9×8 top portion of the matrix is also a Hamming Code, follow the technique used for the Golay Code. The map $x \rightarrow x + 1$ does an interchange of columns and replaces the first with the even parity column. A similar argument invoking cyclicity of the columns proves that the Hamming Code appears in every top 9×7 submatrix.

III. Quadratic Residue Code Properties (Box Codes)

The (63,39;7) binary cyclic code when extended by adding a row/column of odd and even parity has the weight structure of the extended (80,40;16) Quadratic Residue (QR) Code but is not isomorphic to it.

A. Constructions

The (80,39;16) in 10×8 matrix form is obtained from the (63,39;7) cyclic code by adjoining row and column even parity. The cyclic code here is expressed as a 9×7 matrix with entries in the (i, j) positions, $0 \leq i \leq 6$, $0 \leq j \leq 8$

corresponding to the coordinates $9i + 7j \bmod 63$ of the code.

Let **A** be the (63,39;7) cyclic code. The MS polynomial for a code word $\mathbf{a} \in \mathbf{A} = (a_i;\ i = 0 \ldots 62)$ is given by

$$P(z) = C_0 + \sum \text{Tr } C_i z^i + \sum \text{Tr}' \ C_j z^j + C_{21} z^{21} + C_{21}^2 z^{42}$$

where $C_i \in GF(64)$; $i = 1, 3, 5, 7, 13$; $C_j \in GF(8)$; $j = 9, 27$; and

$$\text{Tr}' \ a = a + a^2 + a^4;\ a \in GF(8)$$

Let $z \in GF(64)$ be a primitive root of $GF(64)$. Express $z = xy$ where

$$x = \beta^{9i},\ 0 \le i \le 6;\ y = \beta^{7j},\ 0 \le j \le 8$$

then

$$\text{Tr } Cz = \text{Tr } Cxy = \text{Tr}' \ [Cy + (Cy)^8]x$$

$$\text{Tr } C_3 z^3 = \text{Tr}' \ [C_3' y^6 + C_3'^8 y^3] x^6$$

$$C_3' = C_3^2$$

Replacing the letter by its primed letter to indicate a missing appropriate power,

$$\text{Tr } C_5 z^5 = \text{Tr}' \ (C_5' y^2 + C_5'^8 y^7) x^6$$

$$\text{Tr } C_7 z^7 = \text{Tr } C_7' y \text{Tr } C_9 z^9 = \text{Tr}' \ C_9' x$$

$$\text{Tr } C_{13} z^{13} = \text{Tr}' \ (C_{13} y^4 + C_{13}^8 y^5) x^6$$

$$\text{Tr } C_{27} z^{27} = \text{Tr}' \ C_{27} x^6$$

$$C_{21} z^{21} = C_{21} y^{21}$$

Write the cyclic code in all 39 dimensions as

$$C_0 + \text{Tr } C_7' y^7 + C_{21}' y^{21} + C_{21}'^2 y^{42}$$

$$+ \text{Tr}' \ (C_9' + Cy + C^8 y^8) x + \text{Tr}' \ (C_{27} + C_3' y^6 + C_3'^8 y^3$$

$$+ C_5' y^2 + C_5'^8 y^7 + C_{13} y^4 + C_{13}^8 y^5) x^6$$

where $C_i \in GF(64)$; $i = 1, 3, 5, 7, 13$; $C_j \in GF(8)$; and $j = 9, 27$. The generator polynomial for the code is

$$f_1(z) f_3(z) f_5(z) f_{13}(z)$$

where $f_i(z)$ is the irreducible polynomial over $GF(2)$ with β^i a root.

The weight, $w(\mathbf{a}) \bmod 4$ for even weight words $\mathbf{a}(C_0 = 0)$ is given by $w \bmod 4 = 2\Gamma_2(P_\mathbf{a}(x))$ where $\Gamma_2(P_\mathbf{a}(x)) = \sum_i C_i C_{-i} = \text{Tr}' \ (C_7^9 + C_9 C_{54} + C_{21}^3)$ [2].

Now place the code words in 9×7 matrices (b_{ij}), $0 \le i \le 6$, $0 \le j \le 8$ corresponding to their values $9i + 7j \bmod 63$. Note that the coefficient of x in the above expression is a (9,3;7) code over $GF(8)$, and the coefficient of x^6 is a (9,7;3) RS Code over $GF(8)$. The values $C_0 + \text{Tr } C_7' y^7 + C_{21}' y^{21} + C_{21}'^2 y^{42}$ taken over y form a (9,9;1) binary code. The minimum weight of this code is clearly 7. If the coefficient of x and x^6 is zero, then the minimum weight is given by a weight one word (the coefficient of x) in the (9,9,1) code giving rise to a weight 7 word. If the coefficient of x^6 is nonzero, again there is a minimum weight 12 word, but, complemented by the constants, this can give rise to weight 9 at least.

Now extend the 9×7 matrix into a 10×8 matrix by adjoining even parity rows and columns. The 10th parity row is clearly the code word in MS form $C_0 + \text{Tr}' \ (C_9 x + C_{27} x^6)$. The coefficients $C_0 + \text{Tr } C_7' y^7 + C_{21}' y^{21} + C_{21}'^2 y^{42}$ in the row MS polynomials for $y^{10} = y$ now form a $(10, 9; 2)$ binary code. The coefficient of x is also a $(10, 3; 8)$ code over $GF(8)$. The coefficient of x^6 is a $(10, 7; 4)$ code over $GF(8)$. Adding the even parity column guarantees that the minimum weight w of the expanded code w equals 16.

Note that in the 10th row, $\Gamma_2 = \text{Tr}' \ (C_9 C_{54})$. In the eighth column, $\Gamma_2 = \text{Tr}' \ (C_7^9 + C_{21}^3)$. Thus coming from the length 63 cyclic code with $\Gamma_2 = \text{Tr}' \ (C_7^9 + C_9 C_{54} + C_{21}^3)$ by adjoining a row and column of equal even parity, one has obtained a code with weights equal to 0 mod 4.

The 40th dimension of the constructed code is obtained by adding odd parity row and column to the code words

and keeps the minimum weight and Γ_2 property. This new code has weights 16, 20, 24, 28, 32, 36, 40, 48, 56, and 64 and is self-dual. This is sufficient to guarantee that this code has the weight structure of the (80,40;16) extended QR Code [3].

B. Decoding

Place the code in its 10×8 box and compute row and column parities. Decide whether the code word is of even or odd row/column parity. If in doubt, assume first even and then try odd. Where a row is determined to have an odd number of errors, mark that row as an erasure. Otherwise assume an even number of errors in that row. To correct seven errors, there are at least three rows that must be correct, if seven row erasures are assumed. The coefficient of x is a (10,3;8) code, so one can extract that and generate a correct version. This leaves ten rows that are assumed to be BCH-Hamming Codes.

Only seven of these must be corrected to generate the entire word. Thus, if there is more than one error in each of four rows, but an odd number in the other three, then, with trial and error, $4 + 3 \times 3 = 13$ errors of a particular pattern can be corrected. If the 7-8-9 error patterns are such that three rows are clean, and at least four have single errors, then one can generate the (10,3;8) code over $GF(8)$ the coefficient of x and the (10,7;4) code over $GF(8)$ the coefficient of x^6. The rest emerges easily although this may require assuming first even and then odd parity of the row/column received code words. In general for error patterns of four or less, the row/column parity will be clear and the decoding simplified. In the event of even error patterns in the rows, one will have to decode the (10,3;8) code with some kind of modified RS decoding.

References

[1] G. Solomon and M. M. Sweet, "A Golay Puzzle," *Trans. Info. Theory*, vol. IT-29, no. 1, pp. 174–175, January 1983.

[2] G. Solomon and R. J. McEliece, "Weights of Cyclic Codes," *J. Comb. Theory*, vol. 1, no. 4, pp. 459–475, December 1966.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, New York: North-Holland Publishing Co., 1977.